CLAIMS

1. A method of transmitting data securely over a computer network, comprising the steps of:

(1) establishing a communication path between a first computer and a second computer;

(2) encrypting and transmitting data records between the first computer and the second computer using an unreliable communication protocol, wherein each data record is encrypted without reference to a previously transmitted data record; and

(3) in the second computer, receiving and decrypting the data records transmitted in step (2) without reference to a previously received data record.

2. The method of claim 1, further comprising the step of, prior to step (1), establishing a reliable communication path between the first computer and the second computer and exchanging security credentials over the reliable communication path.

3. The method of claim 2, wherein the step of exchanging security credentials comprises the step of exchanging an encryption key that is used to encrypt the data records in step (2).

4. The method of claim 1, wherein step (2) comprises the step of incorporating a nonce in each data record that is used by the second computer in combination with a previously shared encryption key to decrypt each of the data records in step (3).

5. The method of claim 4, wherein the nonce comprises a random number.

6. The method of claim 4, further comprising the step of, in the second computer, verifying that the nonce has not previously been received in a previously transmitted data record.

7. The method of claim 1,

wherein step (2) comprises the step of embedding an indicator in each of the data records indicating that the data records are encrypted according to an encryption scheme that encrypts records without regard to any previously transmitted data records, and

wherein step (3) comprises the step of determining whether the indicator is present in each record and, in response to determining that the indicator is not present, processing each such record differently than if the indicator is set.

8. The method of claim 1, wherein step (1) is performed using the Transmission Control Protocol, and wherein step (2) is performed using the User Datagram Protocol.

9. The method of claim 1, wherein step (2) is performed by a proxy server that encrypts data records received from another server.

10. A method of securely transmitting a plurality of data records between a client computer and a proxy server using an unreliable communication protocol, comprising the steps of:

(1) establishing a reliable connection between the client computer and the proxy server;

(2) exchanging encryption credentials between the client computer and the proxy server over the reliable connection;

(3) generating a nonce for each of a plurality of data records, wherein each nonce comprises an initialization vector necessary to decrypt a corresponding one of the plurality of data records;

(4) using the nonce to encrypt each of the plurality of data records and appending the nonce to each of the plurality of data records;

(5) transmitting the plurality of data records encrypted in step (4) from the client computer to the proxy server using an unreliable communication protocol; and

(6) in the proxy server, decrypting each of the plurality of encrypted data records using a corresponding nonce extracted from each data record and a previously shared encryption key.

11. The method of claim 10, wherein step (6) comprises the step of checking to determine whether each data record received from the client computer is formatted according to a secure unreliable transmission format and, if a particular record is not formatted according to a secure unreliable transmission format, bypassing the decryption using the corresponding nonce.

12. The method of claim 10, wherein step (3) comprises the step of generating a random number as each nonce.

13. The method of claim 10, wherein step (1) is performed using Transmission Control Protocol, and wherein step (5) is performed using User Datagram Protocol.

14. The method of claim 10, wherein step (6) is performed using an encryption key previously shared using a reliable communication protocol.

15. The method of claim 14, wherein the reliable communication protocol is Transmission Control Protocol.

16. A system for securely transmitting data using an unreliable protocol, comprising:

a first computer comprising a communication protocol client function operable in conjunction with an application program to transmit data records securely using an unreliable protocol; and

a second computer coupled to the first computer and comprising a communication protocol server function operable in conjunction with the communication protocol client function to receive data records securely using the unreliable communication protocol,

wherein the communication protocol client function encrypts each data record using a nonce and an encryption key and appends the respective nonce to each of the encrypted data records; and

wherein the communication protocol server function decrypts each of the data records using the respectively appended nonce and the encryption key.

17. The system of claim 16, wherein the communication protocol client function exchanges encryption credentials with the communication protocol server function using a reliable communication protocol.

18. The system of claim 17, wherein the unreliable communication protocol comprises the User Datagram Protocol, and wherein the reliable communication protocol comprises the Transmission Control Protocol.

19. The system of claim 16, wherein the communication protocol client function and the communication protocol server function are compatible with the SOCKS communication protocol.

20. The system of claim 16, wherein the communication protocol client function and the communication protocol server function are compatible with the SSL/TLS communication protocol.

21. The system of claim 16, wherein the second computer comprises a proxy server that forwards decrypted records received from the first computer to a server computer.

22. The system of claim 16, wherein the second computer comprises a record detector that determines whether an indicator has been set in each data record received from the first computer and, if the indicator has not been set, bypassing decryption in the server computer.